11 – La cryptographie (d'aujourd'hui et) de demain

Motivation

- la cryptographie actuelle est garante de bien des secrets, mais la recherche dans ce domaine n'a jamais été aussi active
- les techniques mathématiques sont sans cesse améliorées : par exemple, les courbes elliptiques se sont déjà substituées aux groupes finis classiques pour plus de robustesse
- pour l'instant, tout repose sur les connaissances actuelles en théorie de la complexité (*i.e.* la complexité des problèmes)
- la cryptographie est aussi largement dépendante du progrès des ordinateurs
- un ordinateur quantique remettrait en cause toute la cryptographie asymétrique actuelle
- pour l'instant, seuls des calculs sur peu de qubits ont été réalisés en pratique
- mais en théorie, des algorithmes quantiques existent déjà qui compromettent la cryptographie actuelle
- en effet, qu'adviendra-t-il le jour où on pourra factoriser un grand entier en temps polynomial ?

> *le challenge RSA consistait jusqu'en 2007 à offrir des prix pour « casser » des entiers-RSA.*

Challenge RSA

RSA number	Decimal digits	Binary digits	Cash prize offered	Factored on	Factored by
RSA100	100	330	US$1,000[8]	April 1, 1991[9]	Arjen K. Lenstra
RSA110	110	364	US$4,429[8]	April 14, 1992[9]	Arjen K. Lenstra and M.S. Manasse
RSA120	120	397	US$5,898[8]	July 9, 1993[10]	T. Denny *et al.*
RSA129 [a]	129	426	US$100	April 26, 1994[9]	Arjen K. Lenstra *et al.*
RSA130	130	430	US$14,527[8]	April 10, 1996	Arjen K. Lenstra *et al.*
RSA140	140	463	US$17,226	February 2, 1999	Herman te Riele *et al.*
RSA150	150	496		April 16, 2004	Kazumaro Aoki *et al.*
RSA155	155	512	US$9,383[8]	August 22, 1999	Herman te Riele *et al.*
RSA160	160	530		April 1, 2003	Jens Franke *et al.*, University of Bonn
RSA170 [b]	170	563		December 29, 2009	D. Bonenberger and M. Krone [c]
RSA576	174	576	US$10,000	December 3, 2003	Jens Franke *et al.*, University of Bonn
RSA180 [b]	180	596		May 8, 2010	S. A. Danilov and I. A. Popovyan, Moscow State University[11]
RSA190 [b]	190	629		November 8, 2010	A. Timofeev and I. A. Popovyan
RSA640	193	640	US$20,000	November 2, 2005	Jens Franke *et al.*, University of Bonn
RSA200 [b] ?	200	663		May 9, 2005	Jens Franke *et al.*, University of Bonn
RSA210 [b]	210	696		September 26, 2013[12]	Ryan Propper
RSA704 [b]	212	704	US$30,000	July 2, 2012	Shi Bai, Emmanuel Thomé and Paul Zimmermann
RSA220 [b]	220	729		May 13, 2016	S. Bai, P. Gaudry, A. Kruppa, E. Thomé and P. Zimmermann
RSA230 [b]	230	762		August 15, 2018	Samuel S. Gross, Noblis, Inc.
RSA232 [b]	232	768		February 17, 2020[13]	N. L. Zamarashkin, D. A. Zheltkov and S. A. Matveev.
RSA768 [b]	232	768	US$50,000	December 12, 2009	Thorsten Kleinjung *et al.*[14]
RSA240 [b]	240	795		Dec 2, 2019[15]	F. Boudot, P. Gaudry, A. Guillevic, N. Heninger, E. Thomé and P. Zimmermann
RSA250 [b]	250	829		Feb 28, 2020[16]	F. Boudot, P. Gaudry, A. Guillevic, N. Heninger, E. Thomé and P. Zimmermann
RSA260	260	862			
RSA270	270	895			

(source wikipédia)

Courbes elliptiques : introduction

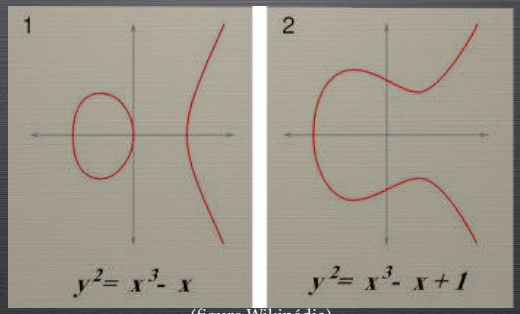
- la cryptographie asymétrique comme RSA ou El Gamal requiert le calcul de l'exponentielle modulaire dans des corps dont les paramètres ont plus de 1000 bits
  - l'arithmétique des processeurs doit être poussée en 32 ou 64-bits
  - la grande taille des paramètres devient critique pour leur stockage dans des systèmes embarqués
- il existe aussi des algorithmes sous-exponentiels pour résoudre le problème du logarithme discret sur les nombres
- pour plus de sécurité, on a besoin de trouver des corps ou même des groupes plus petits
- les courbes elliptiques (*Elliptic Curves*) ont été introduites en cryptographie en 1985 indépendamment par N. Koblitz et V. Miller
- la cryptographie sur les c.e. utilise un groupe de points plutôt que d'entiers dont la taille des coefficients varie de 160 à 256 bits
- les courbes elliptiques garantissent donc la robustesse du chiffrement pour un nombre de bits relativement limité
- bien entendu, Open SSL comporte la commande standard `ec` pour leur mise en œuvre.

Courbes elliptiques : définition

- une courbe elliptique sur $\mathbb{R}$ est un ensemble de points défini par une équation de Weierstrass (simplifiée) :

$$E : \quad y^2 = x^3 + ax + b$$

- les paramètres a et b donnent la forme exacte de la courbe dans le plan
- avec $a, b \in \mathbb{R}$, une courbe elliptique est de la forme :



(figure Wikipédia)

- les c.e. peuvent être définies sur différents corps (les réels, les complexes) mais aussi sur des corps finis
- en cryptographie, on utilise les c.e. sur $\mathbb{F}_p$, p premier (*i.e.* les entiers *modulo* p).

Courbes elliptiques sur $\mathbb{F}_p$

- une courbe elliptique sur $\mathbb{F}_p$, $p > 3$, est un ensemble de points (x, y) de $(\mathbb{F}_p)^2$ vérifiant :

$$y^2 = x^3 + ax + b \mod p$$

assorti d'un élément neutre 0 (point à l'infini)
avec $a, b \in \mathbb{F}_p$ (et sous certaines conditions du discriminant)

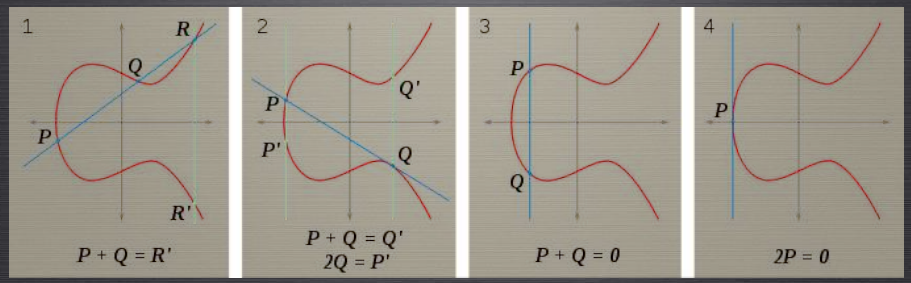
- ces points avec 0 forme un groupe abélien
- l'opposé du point $P(x, y)$ est le point $P(x, -y)$
- on définit l'addition de 2 points distincts ou non :

$$P + Q = R \Leftrightarrow (x_P, y_P) + (x_Q, y_Q) = (x_R, y_R)$$

(cf. interprétation géométrique)

- les points rationnels de la courbe E sont ici les points pour lesquels les coefficients $a, b \in \mathbb{F}_p$.

Interprétation géométrique



(source wikipédia)

Elliptic Curve Discrete Logarithm Problem (ECDLP)

- le problème du logarithme discret transposé sur les c.e. est difficile
- soit un élément primitif P et un autre élément T d'une courbe elliptique E, le problème consiste à trouver l'entier d avec $1 \leq d \leq card(E)$ tel que :

$$P + P + ... + P = d\,P = T$$

- les cryptosystèmes reposent sur le fait que d secret et grand ne pourra pas être calculé facilement
- si d est connu, on a une méthode efficace pour calculer le point $d\,P$
- par suite, l'algorithme d'El Gamal, le protocole d'échange de clef de Diffie-Hellman ainsi que la signature DSA sont transposables sur les courbes elliptiques
- cependant, le chiffrement se transpose moins facilement que la signature ou l'échange de clefs
- les courbes elliptiques sont également utilisées pour factoriser (compliqué) ou pour générer des nombres aléatoires.

Elliptic Curve Diffie-Hellman Key Exchange (ECDH)

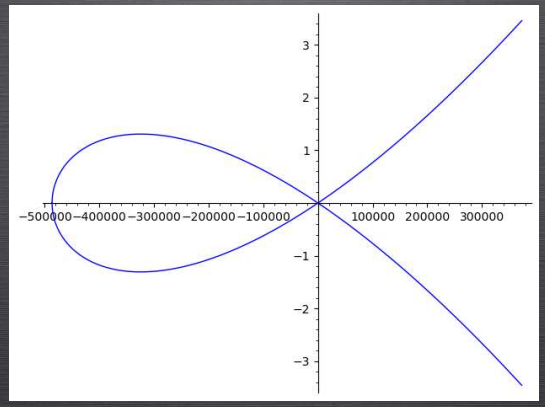
Partage d'un secret

1. Alice et Bob se mettent d'accord publiquement sur un grand nombre premier p, une courbe elliptique E et un point $P = (x_p, y_p)$ appropriés (on note $e = \text{card}(E)$)
2. Alice choisit un nombre $a \in \{2, \ldots, e-1\}$ qu'elle garde secret
3. Alice transmet publiquement à Bob $A = aP = (x_A, y_A)$
4. Bob choisit de même un nombre $b \in \{2, \ldots, e-1\}$ qu'il garde secret
5. Bob transmet publiquement à Alice $B = bP = (x_B, y_B)$
6. le point $\boxed{aB = bA = T_{AB} = (x_{AB}, y_{AB})}$ constitue un secret commun

Une des coordonnées de T_{AB} passée par une fonction de hachage peut ainsi servir de clef secrète partagée en cryptographie symétrique.

Sans transition ...

ECDH : curve 25519



(source wikipédia)

$$y^2 = x^3 + 486662\,x^2 + x$$
$$\textit{modulo } p = 2^{255} - 19$$

Physique quantique

- le prix Nobel Richard Feynman a observé en 1982 que certains phénomènes de mécanique quantique ne pouvaient pas être simulés efficacement par des ordinateurs classiques
- il suggéra que ceci pouvait peut-être être utilisé à l'envers en utilisant les phénomènes quantiques pour faire des calculs jusqu'alors impossibles sur un ordinateur
- en 1994, Peter Shor des ATT-Labs a présenté un algorithme quantique capable de factoriser un entier en temps polynomial si jamais un ordinateur quantique était construit
- les phénomènes de mécanique quantique sont particulièrement contre-intuitifs
- ils ont lieu à l'échelle atomique, ce qui n'est pas directement observable
- pour avoir des particules observables, on opte pour les photons (*cf.* expérience des fentes de Young, 1801)
- aujourd'hui, des Fibres Optiques Photoniques (FOP) sont même dédiées au transport de photons.

Mécanique quantique

- un photon est représenté par un vecteur-unité dans un espace complexe à 2 dimensions
- cet espace est muni d'un produit :

$$(a,b)\cdot(c,d) = a\,\bar{c} + b\,\bar{d}$$

où $\bar{c}$ et $\bar{d}$ sont les conjugués

- la longueur du vecteur (a,b) est donc $(a,b)\cdot(a,b) = |a|^2 + |b|^2$

- on choisit une base pour cet espace : $|\uparrow\rangle$ et $|\rightarrow\rangle$
- une polarisation se représente par : $a\,|\uparrow\rangle + b\,|\rightarrow\rangle$ où $a,b \in \mathbb{C}$

- *passer au travers* d'un filtre revient à mesurer la polarité $\uparrow$ ou bien la polarité $\rightarrow$ d'un photon
- il y a 2 possibilités :
  (1) le filtre est aligné avec le photon
  (2) le filtre est à 45° par rapport au photon

Mécanique quantique (suite)

(1) la probabilité que le photon $a\,|\uparrow\rangle + b\,|\rightarrow\rangle$ ait une polarité verticale est $|a^2|$ et une polarité horizontale $|b^2|$

(2) cela revient à mesurer un photon verticalement aligné avec un filtre à 45° et comme :

$$|\uparrow\rangle = \frac{1}{\sqrt{2}}\,|\nwarrow\rangle + \frac{1}{\sqrt{2}}\,|\nearrow\rangle$$

la probabilité que le photon $1\,|\uparrow\rangle + 0\,|\rightarrow\rangle$ passe au travers du filtre est $(\frac{1}{\sqrt{2}})^2 = 1/2$

- un principe de base de la mécanique quantique est qu'une mesure modifie l'état du photon
- après avoir été mesuré l'état du photon devient ... celui de la mesure

Distribution de clef quantique

- comment faire circuler des bits au travers d'un canal quantique ?
- ces bits peuvent être utilisés pour construire une clef qui sera elle-même utilisée pour faire de la cryptographie symétrique classique

- on se donne un espace 2D de vecteurs complexes
- on choisit une paire de vecteurs orthogonaux de taille 1 appelés $|0\rangle$ et $|1\rangle$
- un bit quantique (quantum bit) dit *qubit* est un vecteur unitaire de cet espace
- les autres qubits sont combinaison linéaire de $|0\rangle$ et de $|1\rangle$
- un qubit est donc représenté par $a\,|0\rangle + b\,|1\rangle$ avec $a,b \in \mathbb{C}$ tels que $|a|^2 + |b|^2 = 1$
- comme pour les photons, on peut mesurer les qubits par rapport à la base $|0\rangle, |1\rangle$

la probabilité d'observer un tel qubit dans l'état $|0\rangle$ *est* $|a|^2$

en 2009, une technique pour échanger une telle clef a été mise en œuvre sur une distance de plus de 250 km en utilisant des câbles de fibre optique

depuis 2000, le protocole d'Ekert concurrence le protocole historique BB84.

Protocole Benett-Brassard (BB84)

- pour communiquer, Alice et Bob ont besoin d'un canal quantique et d'un canal classique

Eve ou Melchior sévissent sur le canal quantique aussi bien que sur le classique ...

- Alice débute la communication en envoyant une suite de bits à Bob
- ils sont encodés dans une base choisie aléatoirement pour chaque bit
- il y a 2 bases : $B_1 = \{|\uparrow\rangle, |\rightarrow\rangle\}$ et $B_2 = \{|\nwarrow\rangle, |\nearrow\rangle\}$
- si Alice choisit B_1 elle encode 0 en $|\uparrow\rangle$ et 1 en $|\rightarrow\rangle$, de même pour B_2
- chaque fois qu'Alice envoie un photon, Bob choisit aléatoirement de le mesurer avec B_1 ou B_2
- Bob garde ses mesures pour lui mais revèle à Alice la séquence des bases qu'il a choisie
- Alice lui répond en lui indiquant quelles bases étaient correctes pour la polarité des photons envoyés
- ils conservent les bits pour lesquels les bases coïncident, jettent les autres
- à peu près la moitié des bases seront conservées
- ils peuvent utiliser ces bits comme clef secrète et faire de la cryptographie symétrique classique avec.

Protocole BB84 : exemple

$B_1 = \{|\uparrow\rangle, |\rightarrow\rangle\}$ schématisée ⇿

$B_2 = \{|\nwarrow\rangle, |\nearrow\rangle\}$ schématisée ⤫

- Alice envoie une suite de bits à Bob encodés dans la base choisie
- Bob choisit aléatoirement de mesurer chaque photon avec B_1 ou B_2
- il revèle à Alice sa séquence de bases et Alice lui indique les bases correctes
- ils conservent les bits pour lesquels les bases coïncident comme clef secrète

Suite de bits d'Alice	0	1	1	1	0	0	1	0
Bases d'Alice	⇿	⤫	⇿	⇿	⤫	⤫	⇿	⤫
Polarisateurs d'Alice	↑	↗	→	→	↖	↖	→	↖
Analyseur de Bob	⤫	⤫	⤫	⇿	⤫	⇿	⇿	⤫
Mesures de Bob	↖	↗	↖	→	↖	↑	→	↖
Secret		1		1	0		1	0

Algorithme quantique

- les ordinateurs quantiques étaient encore limités récemment car on ne manipulait que quelques qubits mais les progrès sont fulgurants
- l'idée pour concevoir des algorithmes quantiques est de faire en sorte que les résultats recherchés apparaissent avec une plus grande probabilité que les autres
- le jour où les écueils techniques seront dépassés, l'impact sur la cryptographie sera énorme
- par exemple, l'algorithme de Peter Shor conduirait à factoriser un grand entier n en temps $\mathcal{O}((\log_2 n)^3)$

  En 2001, IBM *factorise 15 avec un calculateur quantique à 7 qubits selon l'algorithme de Shor*

- le but de cet algorithme probabiliste est de trouver un facteur p de n donné
- l'algorithme de Shor est en 2 parties :
  1. une réduction du problème de factorisation en un problème de recherche d'ordre, faisable sur un ordinateur classique
  2. un algorithme quantique pour résoudre ce problème de recherche de l'ordre d'un élément dans un groupe fini.

Algorithme de Shor

Partie classique (non-quantique) :

1. prendre un nombre pseudo-aléatoire $a < n$
2. calculer $\text{pgcd}(a, n)$
3. si $\text{pgcd}(a, n) \neq 1$, alors $a \mid n$ fin
4. sinon, utiliser le sous-programme quantique de recherche de période pour trouver r, la période de la fonction suivante :

   $$f(x) = a^x \mod n$$

   c'est-à-dire le plus petit entier r pour lequel $f(x + r) = f(x)$
5. si r est impair, retourner à l'étape 1
6. si $a^{r/2} \equiv -1 \mod n$, retourner à l'étape 1
7. sinon $\text{pgcd}(a^{r/2} - 1, n)$ et $\text{pgcd}(a^{r/2} + 1, n)$ sont des facteurs de n fin

Partie quantique : *(...)*

Algorithme de Shor : justification partielle

De l'ordre r de a dans $\mathbb{Z}_n$ à la factorisation de n :

- r est le plus petit entier tel que $a^r \equiv 1 \mod n$ donc

  $$n \mid (a^r - 1)$$

- r est pair :

  $$a^r - 1 = (a^{r/2} - 1)\,(a^{r/2} + 1) \equiv 0 \mod n$$

  et donc

  $$n \mid (a^{r/2} - 1)\,(a^{r/2} + 1)$$

- d'une part d'après la minimalité de r, d'autre part du fait du 6. :

  $$n \nmid (a^{r/2} - 1) \quad \text{et} \quad n \nmid (a^{r/2} + 1)$$

- en passant par l'identité de Bézout, on obtient 2 facteurs de n :

  $$\text{pgcd}(a^{r/2} - 1, n)$$

  $$\text{pgcd}(a^{r/2} + 1, n)$$

Cryptographie post-quantique

Prête à entrer en lice aux côtés de la cryptographie classique :

- *février 2016* : le NIST lance un appel pour trouver des algorithmes qui résistent à l'ordinateur quantique
- *juillet 2020* : 7 « finalistes » attaquent mutuellement leurs algorithmes pour les tester
- *juillet 2022* : 4 algorithmes retenus et d'autres en secours
  chiffrement : Crystals-Kyber
  signature :
  - Crystals-Dilithium
  - Falcon
  - Sphincs +

FIN !

En savoir plus ...
A part Sphincs +, tous sont basés sur les réseaux arithmétiques,

Un an encore est nécessaire à la standardisation des protocoles en vue d'une cohabitation avec les algorithmes cryptographiques pré-quantiques.